UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,496	10/29/2001	Carey Nachenberg	20423-05957	3384

45969 7590 11/02/2005

SONNENSCHEIN NATH & ROSENTHAL LLP
FOR SYMANTEC CORPORATION
P. O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/046,496	NACHENBERG ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17 and 20-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17 and 20-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/17/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 8/17/2005.

All objections and rejections not set forth below have been withdrawn.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Applicants have amended claims 1, 2, 12, 13, 20, 22, 27, 28, and 30 – 33 to include limitations for the "automatically" generating of an access control time or the "automatically" generating of a virus alert time. Furthermore, these claims have also been amended to include the limitations of a "real time" determination of computer content executability. These added limitations are not described nor find support in the specification as presented.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1 – 17 and 20 – 33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. See objection to specification above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 – 10 and 12 – 33 is rejected under 35 U.S.C. 102(e) as being anticipated by Bates et al., U.S. Patent 6,721,721 B1.

Regarding claim 1, Bates et al. discloses:

entering a first computer virus status mode in response to a first computer virus outbreak report (Bates et al., col. 1, lines 13-52). Bates et al. reports the outbreak of new and more sophisticated viruses. The invention as disclosed by Bates et al. is for the purpose of protecting against these outbreaks.

automatically generating a first computer virus alert time corresponding to entry into the first computer virus status mode (Bates et al., fig. 7, elem. 214; col. 7, lines 20-35); Bates et al. discloses a method for accessing computer content on a local machine or on a network. Content is filtered based upon a generated virus alert time entered by a user in a virus status mode defined by the user. Furthermore, Bates et al. discloses an administrator providing time control parameters the system in a human-readable form (Arabic numerals) via an input means, such as a keyboard. However, these human-readable control parameters are "automatically" converted into meaningful computer-readable form for the system to act upon.

comparing a time stamp of a computer content with the first computer virus alert time (Bates et al., col. 12, lines 59-65);

and determining in real time the executability of the computer content in response to the result of the comparing step (Bates et al., col. 9, line 56 – col. 10, line 8). Bates et al. discloses that in response to a comparison, a determination of computer content executability is performed. This determination to executed computer content is made in real time.

Regarding claim 2, Bates et al. discloses:

automatically generating a first access control time based on the first virus outbreak report (Bates et al., fig. 7, elem. 214). The system of Bates et al. takes human input and "automatically" generates computer readable parameters.

and converting the first access control time into the first virus alert time (Bates et al., fig. 7, elem. 214; col. 12, lines 59-62). A "prior point in time" ("virus alert time") is derived from the period of time specified by element 214 ("access control time") and is compared to the timestamp of the file.

Regarding claim 3, Bates et al. discloses:

wherein the first access control time is a relative time stamp (Bates et al., fig. 7, elem. 214; col. 12, lines 59-62). A "prior point in time" ("virus alert time") is derived from the period of time specified by element 214 ("access control time") and is relative in time.

Regarding claim 4, Bates et al. discloses:

wherein the first access control time is a pre-determined time period for access control under the first computer virus status mode (Bates et al., fig. 7, elem. 214). The access control time is pre-determined by the user.

Regarding claim 5, Bates et al., discloses:

determining the presence of a value representing the computer content in a memory table of executable computer content (Bates et al., col. 7, lines 12-34).

Regarding claim 6, Bates et al., discloses:

wherein the computer content is not executed when the value representing the computer content is not present in the memory table of executable computer content (Bates et al., col. 11, lines 11-24; col. 3, lines 24-27). As disclosed by Bates et al., content not present in the memory table of executable computer content is flagged as untrustworthy. The invention as disclosed by Bates et al. is configurable to eliminate untrustworthy computer content from the list of accessible content, thus not providing access to the content for execution.

Regarding claim 7, Bates et al. discloses:

wherein the value is a hash value of the computer content (Bates et al., col. 12, lines 55-58).

Regarding claim 8, Bates et al. discloses:

wherein the computer content is executed only when the computer content is time stamped prior to the first computer virus alert time (Bates et al., col. 13, lines 42-59; col. 3, lines 24-27). Computer content that is time stamped prior to the first computer virus alert time is branded as trustworthy. Thus, the content would not be subjected to denial of access for execution.

Regarding claim 9, Bates et al. discloses:

entering types of computer codes that should be blocked from execution in response to the first computer virus outbreak report (Bates et al., col. 9, line 62 – col. 10, line 28);

and blocking execution of a computer code that belongs to the entered types of computer codes (Bates et al., col. 3, lines 24-27). The invention as disclosed by Bates et al. is configurable to eliminate untrustworthy computer content from the list of accessible content, thus not providing access to the content for execution.

Regarding claim 10, Bates et al. discloses:

generating a second virus alert time in response to a second computer virus outbreak report; comparing the time stamp of the computer content with the second computer virus alert time; determining the executability of the computer content in response to the result of comparing the time stamp of the computer content with the second computer virus alert time (Bates et al., col. 3, lines 5 – 15). The above limitations of claim 10 are essentially similar to claim 1 with the exception that they are directed to a second instance of the method of claim 1. Bates et al. discloses that the method of claim 1 produces a set of results. Thus, Bates et al. discloses a secondary instance of the method of claim 1, as a the word "set" dictates more than a singular occurrence of the method of claim 1.

performing antivirus processing upon the computer content (Bates et al., col. 9, lines 62-66). Bates et al. discloses the processing of computer content for the likelihood of existing viruses.

Regarding claim 12, Bates et al. discloses:

an access control console, for entering a first computer virus status mode and for recovering a preselected virus access control time corresponding to said virus status mode (Bates et al., fig. 1, elem. 33; fig. 7);

an anti-virus module, coupled to the access control console, configured to automatically generate a virus alert time based on the virus access control time and to compare a time stamp of a target computer content with the virus alert time prior to execution of the target computer content (Bates et al., fig. 1, elem. 30; see rejections of claims 1 and 2).

Regarding claim 13, Bates et al. discloses:

a memory module for storing time stamps of the plurality of computer contents (Bates et al., fig. 1, elem. 46);

and an access control module, coupled to the access control console and to the memory module, for automatically generating the virus alert time and for comparing the time stamp of each target computer content with the virus alert time (Bates et al., fig. 1, elem. 42; see rejections of claims 1 and 2).

Regarding claim 14, Bates et al. discloses:

a computer virus processing module, coupled to the access control module, for further processing a target computer content in order to determine the executability of the target computer content (Bates et al., fig. 1, elem. 44).

Regarding claim 15, Bates et al. discloses:

wherein the memory module stores a value representing each of the computer contents (Bates et al., col. 12, lines 52-65).

Regarding claim 16, Bates et al. discloses:

wherein the access control module is configured to determine the presence of the value in the memory module as representing a target computer content (Bates et al., fig. 3).

Regarding claim 17, Bates et al. discloses:

wherein the value is a hash value (Bates et al., col. 12, lines 52-65).

Regarding claim 20, Bates et al. discloses:

creating a list of time-stamped executable computer contents (Bates et al., fig. 3, elem. 92).

entering a virus alert mode in response to a virus outbreak report (Bates et al., fig. 2; col. 1, lines 13-52).

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking the execution of suspicious or susceptible computer contents that are time-stamped not before an automatically generated virus alert time, the access control message including a first control parameter for generating the virus alert time (Bates et al., fig. 2; fig. 7; see rejections of claims 1 and 2).

receiving a request to execute a target computer content; and determining the executability of the target computer content based on the access control rule in the access control message (Bates et al., fig. 2).

Regarding claim 21, Bates et al. discloses:

applying anti-virus operation upon each executable computer content, storing a hash value of each executable computer content in the list; and inserting a time stamp corresponding to the moment of storing the hash value of the executable computer content (Bates et al., fig. 3).

Regarding claim 22, Bates et al. discloses:

receiving the access control message; automatically converting the first control parameter into the virus alert time; comparing the time stamp of the target computer content in the list with the virus alert time; and determining in real time the executability

of the target computer content based on the result of the comparing step (Bates et al., fig. 2, fig. 3, fig. 7; see rejections of claims 1 and 2).

Regarding claim 23, Bates et al. discloses:

applying an anti-virus operation upon the target computer content (Bates et al., fig. 3).

Regarding claim 24, Bates et al. discloses:

a second control parameter for specifying types of computer contents that should be subject to the access control rule (Bates et al., col. 9, line 62 – col. 10, line 28);

a third control parameter for specifying an expiration time for the access control rule (Bates et al., fig. 7, elem. 217);

and a fourth control parameter for identifying the access control message (Bates et al., fig. 2).

Regarding claim 25, Bates et al. discloses:

determining validity of the access control message based on the third control parameter (Bates et al., fig. 3);

Regarding claim 26, Bates et al. discloses:

determining executability of the target computer content based on the second control parameter (Bates et al., col. 9, line 62 – col. 10, line 28);

Regarding claims 27 and 28, they are rejected for the same reasons as claims 20 and 22, and further because Bates et al. discloses the usage of their system in a network of communicating computers (Bates et al., fig. 1). Communications to a user can be blocked when computer content is deemed to be untrustworthy (Bates et al., col. 3, lines 24-27, col. 14, line 6 – col. 15, line 8).

Regarding claim 29, Bates et al. discloses:

wherein the data communication is blocked when the target computer content is time-stamped not before the virus alert time (Bates et al., fig. 3; fig 7).

Regarding claim 30, Bates et al. discloses:

a firewall module monitoring data communications initiated by a target computer content and sending a request to examine the data communications (Bates et al., fig. 1, elems.20, 30, 50). Bates et al. discloses that the system is useful in a network and it is capable of filtering trustworthy and untrustworthy computer content – thus, acting as a firewall module.

an access control console, for generating an access control message specifying an access control rule for blocking data communications of the target computer content when said content is time-stamped not before a virus alert time, the access control message including a first control parameter enabling the automatic generation of the virus alert time (Bates et al., fig. 7; fig. 2);

and an access control module, coupled to the access control console and the firewall module, configured to receive the access control message and a request from the firewall module, and to automatically generate the virus alert time based on the virus access control time and to determine whether the data communication should be blocked based on the access control rule (Bates et al., fig. 1, elem. 44, see rejections of claims 1 and 2).

Regarding claim 31, it is a program and computer medium claim implementing the method claim 1, and it is rejected for the same reasons (see also, Bates et al., fig. 1).

Regarding claim 32, Bates et al. discloses:

means for entering a computer virus status mode and for automatically recovering a preselected virus access control time (Bates et al., fig. 7);

coupled to the entering and recovering means, means for automatically calculating a virus alert time based on the virus access control time (Bates et al., fig. 1, elems. 31, 42, 44).

and coupled to the calculating virus alert time means, means for comparing a time stamp of a target computer content with the virus alert time prior to execution of the computer content (Bates et al., fig. 1, elem. 42).

Regarding claim 33, Bates et al. discloses:

means for storing time-stamped executable computer contents (Bates et al., fig. 1, elem. 46);

a firewall means for monitoring data communications occurring to the executable computer contents (Bates et al., fig. 1, elems. 44, 29, 52).

means for entering a computer virus status mode and for automatically recovering a preselected virus access control time (Bates et al., fig. 7);

coupled to the entering and recovering means, means for automatically calculating a virus alert time based on the virus access control time *(Bates et al., fig. 1, elems. 31, 42, 44).*

and coupled to the calculating virus alert time means, the storing means, and the firewall means, means for comparing a time stamp of an executable computer content with the virus alert time to determine whether the data communication occurring to the executable computer content should be blocked (Bates et al., fig. 1, elem. 44, 42).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bates et al., U.S. Patent 6,721,721 B1 in view of Symantec, "Norton AntiVirus Corporate Edition".

Regarding claim 11, Bates et al. discloses that viruses can be found in email attachments, and that it is well known in the art for antivirus programs to have the capability for performing antivirus processing on emails and email attachments (Bates et al., col. 1, lines 35-63). Bates et al. discloses an antivirus program or module for performing such antivirus processing (Bates et al., fig. 1, elems. 44, 52). Bates et al., however, does not disclose the details of the antivirus processing for emails and email attachments. Specifically, Bates et al. does not disclose that the antivirus program or module removes the computer content from the E-mail body, and denies execution of the computer content.

Symantec discloses an antivirus program and the details of how the program performs antivirus processing upon an email with an attachment. Symantec discloses that the antivirus program scans content attached to an email body and removes such content if it is found to contain a virus, thus, denying execution of the content (Symantec, page 15, par. 2; page 22, "Managing Realtime Protection").

It would have been obvious for one of ordinary skill in the art to combine the details disclosed by Symantec for the antivirus processing of emails with the system of Bates et al. because the system of Bates et al. discloses an antivirus program capable of performing antivirus processing for processing of emails.

Response to Arguments

Applicant's arguments filed 8/17/2005 have been fully considered but they are not persuasive.

Applicants argue primarily that:

(i) *Independent claim 1 recites that the first computer virus status mode is entered "in response to a first computer virus outbreak report." This implies that there has been an outbreak of a computer virus (as that term is broadly defined). There is no such outbreak of a computer virus in Bates. The passage of Bates cited by the Examiner on this point (column 1, lines 13-52) is irrelevant, because said passage is a discussion of the prior art.*

In response, the examiner reiterates that Bates clearly reports the outbreak of new and sophisticated viruses. In response to this report, the system of Bates et al. is used to defend and protect against these outbreaks. The applicant has broadly claimed a "virus outbreak report", such as is found in Bates et al. The applicant's argument is unpersuasive.

(ii) *Secondly, claim 1 as amended recites that the first computer virus alert time is*

generated "automatically." This is in sharp contrast to the time entry cited by the Examiner in Bates (Figure 7, item 214), which is a manual (non-automatic) entry entered by a human to help categorize whether a certain file should be considered to be trustworthy or untrustworthy. The passage in Bates (column 7, lines 20-35) cited by the Examiner is not relevant to this issue.

In response to this argument, as was stated with reference to the amended claims above, the examiner asserts that the human inputted control parameters are "automatically" converted or generated into a computer-readable "virus alert time" that is usable by the system.

(iii) *The last two clauses of claim 1 as amended recite that the first computer virus alert time is used in a "real time" determination as to whether the computer content will be executed. This differs from Bates in the following respects. Looking at the passage of Bates cited by the Examiner (column 12, lines 59-65), it is evident that Bates' timestamp is used only to determine whether the file that is being inspected has been changed. If so, it will be virus-scanned. Time information in Bates is used to create virus status information that is stored on a remote server 30 (not within the confines of the network being protected as in the present invention). This virus status information is used subsequently (not in real time as recited in Applicants' claim 1) to determine whether the file is safe to execute or not.*

In response, the applicants allegation "*claim 1 as amended recite that the first computer virus alert time is used in a "real time" determination as to whether the computer content will be executed"* is not the limitation of claim. The limitation as claimed calls for a determination of executability (a determination of a quality), not a determination of whether the computer content will be executed (a determination of an action) as erroneously argued by the applicant. Thus, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., determination of whether the computer content will be executed) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Furthermore, applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections. Specifically, the applicant alleges, "*Time information in Bates is used to create virus status information that is stored on a remote server 30 (not within the confines of the network being protected as in the present invention).* The examiner finds the applicant's argument regarding the location of computer information within a network irrelevant with respect to the applicant's argument regarding the amended limitation of "real time".

Furthermore, the applicant alleges ,"*This virus status information is used subsequently (not in real time as recited in Applicants' claim 1) to determine whether the file is safe to execute or not".* In response, the applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Specifically, as shown above, the applicant does not show any deficiency of the prior art in light of the amendment to include the limitation of "real time".

(iv) *A firewall is not suggested in Bates.*

In response to this argument, the examiner asserts that the applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

The examiner directs the applicant's attention to the reasons of record for the rejection.

(v) *In addition, Applicants' dependent claims contain numerous additional novel features that are not suggested by the prior art. For example, claim 3 recites that the first access control time is a relative time stamp. The relative time stamp overcomes the*

problems of time disparity among different computers on the network, insuring that all said computers receive uniform protection. Specification page 4, paragraph 0010. This relative time stamp is not suggested by the prior art.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a relative time stamp for overcoming problems of time disparity among different network computers) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(vi) *Claims 7, 17, and 21 recite a hash value used to identify computer content. Bates does not suggest a hash value. His CRC is not a hash value. Column 12, lines 55-58.*

In response the examiner directs the applicant's attention to the applicant's own disclosure, which states: "*The hash value ("hash") is a contraction of computer file contents created by applying a hash function*" (Spec, page 18, lines 3,4). A CRC is a value representing a small number of bits, created by applying a hash function to a larger number of bits or a computer file.

(vii) *Claim 24 recites second, third, and fourth control parameters, which enable a huge degree of granularity in defending an enterprise network against real time attacks of malicious computer code. These parameters are not suggested by Bates.*

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

(viii) *The Examiner cites Norton for the recitations of "removing the computer content from the E-mail body" and "denying execution of the computer content." However, the passages of Norton cited by the Examiner do not support these recitations. The passage on page 15 of Norton states: "If the file is cleaned, the virus is successfully and completely removed from the file" i.e., Norton uses the word "removed." However, Norton says that the virus is removed, not that the computer content is removed as recited in claim 11. Similarly, the passage at page 22 of Norton fails to suggest "removing the computer content from the E-mail body." In fact, the passage at page 22 teaches away from this recitation, because it states: "Norton Antivirus scans only the attachments associated with email. There is no need to scan the message itself, as mail messages are not subject to computer viruses."*

Similarly, the two passages of Norton cited by the Examiner do not suggest the recitation of denying execution of the computer content.

The applicant has alleged that the prior art as combined does not teach *the recitations of "removing the computer content from the E-mail body" and "denying execution of the computer content."* To support such allegations, the applicant states, *Norton says that the virus is removed, not that the computer content is removed as recited in claim 11.* The examiner discerns that the applicant is effectively saying that a computer virus is not computer content. Yet, in contradiction, the applicant previously states, "As used herein, "computer virus" broadly includes any and all types of malicious computer code" (Remarks, page 10). The examiner finds the applicant's arguments unpersuasive.

Furthermore, the examiner asserts that the applicant's argument of "teaching away" is also unpersuasive it is directed towards the scanning of email bodies and not content attached to email bodies as is claimed.

Furthermore, the examiner asserts that the complete removal of computer content from a computer environment will prevent the removed computer content from operation within the computer environment that it has been completely removed from.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

"Cyclic redundancy check", Wikipedia, http://en.wikipedia.org/wiki/Cyclic_redundancy_check, accessed 10/31/05.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

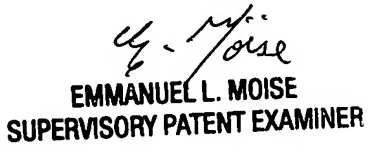
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
Art Unit: 2137



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER